Computer security – assignment 2

Q1) What is the difference between a block cipher and a stream cipher?

A block cipher processes the input one block of elements at a time,

producing an output block for each input block. And the entire block must be

available before processing. A stream cipher processes the input elements

continuously, producing output one element at a time, as it goes along..

Q2) search and find an AES encryption software to encrypt the attached   
plaintext.txt file using the following 128 bits key   
06DB307E28AA3419F0646DAC19F1C593

Where the AES encrypt must use CBC mode. Attach the encrypted file  
ciphertext.txt to the assignment solution + video capture your computer   
screen during the encryption.

Q3) Why do some block cipher modes of operation only use encryption while others use

both encryption and decryption?

Because of its vulnerability to brute-force attack, DES, which only uses encryption, has been largely replaced by stronger encryption schemes. And to preserves the existing investment in software and equipment, stronger encryption schemes are to use multiple encryption with DES and multiple keys.

An obvious counter to the meet-in-the-middle attack is to use three stages of encryption with three different keys. Using DES as the underlying algorithm, backward compatibility with DES is provided.

Q4) What are the three broad categories of applications of public-key cryptosystems?

Key distribution, Digital signatures, Encryption/Decryption.

Q5) What requirements must a public-key cryptosystem fulfill to be a secure algorithm?

The number of bits in the key should be much larger than symmetric crypto keys.

Q6) List the different approaches to attack the RSA algorithm

Brute force key search, mathematical attacks, side-channel attacks, chosen-ciphertext attack.

Q7) Describe the countermeasures to be used against the timing attack.

Use constant exponential time. Whatever the d value is, the exponential time is fixed. (in decryption, there is Cd calculation.)

Add random delays. It makes the attackers hard to guess how much time is needed when calculating Cd.

Blinding. It multiplies the ciphertext by a random value so that attacker cannot know the ciptertext being decrypted.

Q8) What characteristics are needed in a secure hash function?

One-way property, weak collision resistance, strong collision resistance.

Q9) search and find an RSA encryption software to encrypt the attached   
plaintext.txt file using the following 1024 bits key pairs

-----BEGIN PUBLIC KEY-----

MIGeMA0GCSqGSIb3DQEBAQUAA4GMADCBiAKBgHwHgNMBRpSc6PsO5YlaB0NHqmqr

grCXQVDFtjeUUFyb6QwNK3RAO9lF6gZkZKSq03nZLMezjFC5p4oybUqb7ORfLC3E

A0WeZJTZARGDuCTDiAFBAVnQKR1MDU8iv05fKbVHrPNK1DUE1qmTVCPrmrxg50dX

5GfihzeN+3dAO4+fAgMBAAE=

-----END PUBLIC KEY-----

-----BEGIN RSA PRIVATE KEY-----

MIICWgIBAAKBgHwHgNMBRpSc6PsO5YlaB0NHqmqrgrCXQVDFtjeUUFyb6QwNK3RA

O9lF6gZkZKSq03nZLMezjFC5p4oybUqb7ORfLC3EA0WeZJTZARGDuCTDiAFBAVnQ

KR1MDU8iv05fKbVHrPNK1DUE1qmTVCPrmrxg50dX5GfihzeN+3dAO4+fAgMBAAEC

gYBxI08KK5G8ot2Llm0fu7YAU3FK2KTgfTkhexja3jnoIHiXe7P12Vo+uh3eMtnz

s7gw4ECO8mO+h3wi/hjgBBg0fKD+0Drs3EP3jd93+fxvghxmejpPiagx1QveFp0F

8bWUQEvB6QU1bumsBheDt7cDyR7V/vL9Oz+a2096qtgKEQJBALkgLWO9ugf1T8rv

Gh1mfcKG3LSAy0aUvj4qIjZmKaV4/+pXjsHG3TFftNyARyyL4vwQX6RAww2kjjgL

WFSqFD0CQQCrg2I8nnTrxp6N3VJFVeKnKeyWBcCLnnrDdH4CZ82sUr1N6uJi+nTe

GNQebwio2OUx9JWuTtRP13VuY1ajnYULAkBIbH01YxkvWdowkyANVnZmruoTN7vO

zgwrN8KQs6EhWlgMLtrrlkgcs8uG5Cx0EfnoEOPJ14g3gyQcatvQq4UlAkBKYbJK

49WFIyBEGgXB+BtRr8bg0SHN6y8GcRDs7iOuZjue/QytLD1ezJnBkRnKUDYl0hLQ

A3PkJGbTNtWuI3Q9AkBHdcAKIjZzagwGhx0m1T6nfaWyw89tNrNfVFizl9rj4tdh

uROovzs8R+zOHAAcljfI+gLAL716nWV7jpRj1/vV

-----END RSA PRIVATE KEY-----

Note: You can generate your own public and private keys if you do not want to use the above-given keys.

Attach the encrypted file as ciphertext\_RSA.txt to the assignment solution + video capture your computer screen during the encryption.